

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-273705
(43)Date of publication of application : 05.10.2001

(51)Int.Cl. G11B 19/04
G11B 7/004
G11B 7/007
G11B 19/02
G11B 20/10

(21)Application number : 2000-028053 (71)Applicant : SONY CORP
(22)Date of filing : 04.02.2000 (72)Inventor : IIDA MICHIIHIKO

(30)Priority
Priority number : 2000009381 Priority date : 18.01.2000 Priority country : JP

(54) RECORDING MEDIUM ITS IDENTIFYING METHOD AND ITS RECORDING AND REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent altering and forging of important file data such as approval and settlement of accounts of a programmable recording medium.
SOLUTION: In the recording medium its identification method and the recording and reproducing device of the recording medium random analog waveform signals are recorded into a programmable recording medium. The signals are registered as identification data i.e. fingerprint data. The data are transferred to a host computer and stored as a fingerprint intrinsic to a recording medium. During a reprogramming to the medium the fingerprint data stored in the host computer and the fingerprint data of the recording medium are compared and a writing approval is given when the comparison result falls within a prescribed comparison range value.

CLAIMS

[Claim(s)]

[Claim 1] A recording medium being a recording medium in which re-writing is possible having recorded a random waveform pattern in a prescribed data record

section of the above-mentioned recording medium and making with identification data of this recording medium.

[Claim 2] The recording medium according to claim 1 wherein said random waveform pattern is the identification data which shook and acquired a laser power value within a prescribed range value with random data generated by a random number generation means.

[Claim 3] The recording medium according to claim 1 wherein said random waveform pattern is the identification data which shook and acquired a focus bias value in a prescribed range with random data generated by a random number generation means.

[Claim 4] A record step which records a random waveform pattern in a prescribed data record section of a recording medium in which re-writing is possible
A memory step which incorporates a random waveform pattern recorded at the above-mentioned record step is sent out to a host computer and is memorized as identification data to a memory measure in this host computer
A random waveform pattern recorded at the above-mentioned record step at the time of writing to the above-mentioned recording medium is read and sent out to the above-mentioned host computer as digital data -- this host computer -- this -- it being sent out and digital data as compared with identification data within the above-mentioned memory measure
An identifying method of a comparison step which will permit writing to this recording medium if this comparison data is a predetermined value within the limits and a recording medium changing more.

[Claim 5] A recording and reproducing device of a recording medium which is provided with the following and characterized by accomplishing the above-mentioned host computer so that re-write-in permission or disapproval data may be sent out.

A recording device which records a random waveform pattern in a predetermined data writing field of a recording medium in which re-writing is possible.

A reproduction means which reproduces a random waveform pattern recorded by the above-mentioned recording device and is sent out to a host computer.
the above sent out to the above-mentioned host computer -- a random waveform pattern being memorized to this host computer and it being considered as identification data of a recording medium and
A comparison means [host computer / this / this identification data / waveform pattern / which the above-mentioned reproduction means sent out to this host computer at the time of re-writing of a recording medium / random].

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] With respect to a recording medium in which re-writing is

possiblean identifying method for the sameand its recording and reproducing deviceespeciallythis invention is used for the recorder of the recording medium in which re-writing is possibleand relates to a suitable recording mediuman identifying method for the sameand its record re-device.

[0002]

[Description of the Prior Art]From the formersince the copy from various recording media or alteration of computer softwareimage softwarevoice softwareetc. is comparatively easythe prevention measure for preventing these illegal copies and an alteration is taken. These prevention measures record a unique code on the recording medium itself logically or physically fundamentallyalthough many methods are proposedand it is being identified by reading this whether it is an inaccurate or regular recording medium.

[0003]For examplein JPH7-176080Athe recording medium which attained differentiation with the recording medium which was formed by regenerated light by having made into security information the pattern code which can be read at the time of recording-medium creationand was physically copied in the data recording regions of a recording medium and outside the record section is indicated.

[0004]The recording medium which recorded security information logically in the same format to which the usual thing and distinction are not attached using rupture of a hour entry in the buffer space in the inner circumference in a recording-medium management domainand its check device are indicated by JPH8-153342A.

[0005]

[Problem(s) to be Solved by the Invention]RecentlyCD-RW (Compact Disc Rewritable)DVD-RAM (Digital Versatile Disc-RAM)The recording medium in which re-writingsuch as MO (Magnet Optical disc) and magnetic tapeis possibleOr CD-R (Compact Disc Recordable)Recording mediasuch as WORM (Write Once Read Many opticaldisc: write once optical disk)such as DVD-R (Digital Versatile Disc Recordable)have appeared on the market widely. The recording medium which prevented the copy and the alteration by the above-mentioned security information has many which have managed security information with digital data only for reproduction.

[0006]In the recording medium in which above-mentioned re-writing is possibleor a recording medium like WORMwhen recording and electronic-file-izing the important matter which needs recognitionsettlement of accountsattestationetc.an unjust alteration or forgery needs to be made not to be made recordable to the recording medium itselfbut. When putting the identification information as security information into a recording medium physically as mentioned abovemany equipment is needed and the compatibility between marketed recording mediaetc. pose a problem.

[0007]When the identification information as security information was logically put into a recording medium and security information was managed with digital data on the other handsecurity information was decoded theoretically and there was a

problem whose alteration and forgery are attained.

[0008] This invention was made in order to cancel above-stated SUBJECT and it tends to provide a recording medium which recorded the security information which identification information cannot decode easily an identifying method for the same and its recording and reproducing device.

[0009]

[Means for Solving the Problem] A recording medium of the 1st this invention is a recording medium in which re-writing is possible records a random waveform pattern in a prescribed data record section of this recording medium and forms it with identification data of a recording medium.

[0010] A recording medium of the 2nd this invention records identification data which shook and acquired a laser power value within a prescribed range value with random data made to generate the random waveform pattern by a random number generation means.

[0011] A recording medium of the 3rd this invention records identification data which shook and acquired a focus bias value within a prescribed range value with random data made to generate said random waveform pattern by a random number generation means.

[0012] A record step which records a random waveform pattern in a prescribed data record section of a recording medium which the identifying method of a recording medium of this invention can re-write in Incorporate a random waveform pattern recorded at this record step and it sends out to a host computer A memory step memorized as identification data to a memory measure in a host computer A random waveform pattern recorded at a record step at the time of writing to a recording medium is read It sends out to a host computer as digital data and a host computer comprises a comparison step which permits writing to a recording medium if this comparison data is a predetermined value within the limits about this sending-out ***** digital data as compared with identification data within a memory measure.

[0013] A recording device which records a random waveform pattern in predetermined data recording regions of a recording medium which the recording and reproducing device of a recording medium of this invention can re-write in A reproduction means which reproduces a random waveform pattern recorded by this recording device and is sent out to a host computer A host computer memorizes a random waveform pattern sent out to a host computer and uses it as identification data of a recording medium It has a comparison means [host computer / identification data / waveform pattern / which a reproduction means sent out to a host computer at the time of re-writing of a recording medium / random] and a host computer is accomplished so that re-write-in permission or disapproval data may be sent out.

[0014] Since an analog random waveform is recorded as identification data according to the above-mentioned 1st thru/or the 3rd recording medium powerful protection is attained with identification data which is hard to decode as compared with a case where identification data which is security information in digital one is

processed.

[0015]According to the identifying method of an above-mentioned recording mediuman identifying method which cannot alter or forge easily an electronic file which needs recognitionsettlement of accountsetc. is acquired simply.

[0016]If it is a recording and reproducing device which has an optical pickup in which record reproduction is possible for data of a recording medium according to the recording and reproducing device of an above-mentioned recording mediuma recording and reproducing device which can record identification data will be obtained simplywithout forming a special device.

[0017]

[Embodiment of the Invention]Hereafterdrawing 1 thru/or drawing 8 explain the example of 1 gestalt of this invention.

[0018]Drawing 1 shows the distribution diagram of the recording and reproducing device of this inventionand explains the recording and reproducing device of CD-R which is a write once optical disk as a recording medium.

[0019]In drawing 1the recording and reproducing device 28 is connected to the host computer (it is hereafter described as H.CPU) 26 via a busand H.CPU26 has the memory measures 27such as a hard disk drive (HDD).

[0020]Having the recording medium (it is described as CD-R below) 1 in the recording and reproducing device 28this CD-R1 formed the pregroove on the synthetic resin base 1aand it formed the reflecting layers 1csuch as goldon the recording layers 1bsuch as coloring matter of a cyanogen systemand has covered this reflecting layer 1c top with 1 d of protective layers.

[0021]CD-R1 is laid on the turntable 2it rotates with the spindle motor 3and drive controlling of the spindle motor 3 is carried out via the servo circuit 20 and the spindle drive circuit 23.

[0022]By the slide motor 4the optical pickup 5 and the high power laser 6 are made as it is movable to the spoke direction of CD-R1. The slide motor 4 carries out slide - controlling of the optical pickup 5 or the high power laser 6 via the servo circuit 20 and the slide drive circuit 22.

[0023]A writing control signal is supplied to the laser drive circuit 8 through RF amplifier 9 from CPU17 at the time of the re-writing to CD-Rand the high power laser 6 carries out drive controlling of the high power laser 6and the power of the high power laser 6 is monitored by the laser power monitor 7.

[0024]As for the optical pickup 5drive controlling of the control of a focus and the biaxial direction of tracking is carried out via the servo circuit 20 and the biaxial actuator drive circuit 21.

[0025]The RF signal from RF amplifier 9 and the control signal from CPU17 are supplied to the servo circuit 20. The catoptric light taken up by the optical pickup 5 is changed into an electrical signaloutputs an RF signal via RF amplifier 9and is supplied to the RF processing circuit 10.

[0026]An RF signal carries out an EFM (8 -14 abnormal conditions) recovery after synchronous detection in the synchronous detection circuit 12 via the PLL (Phase Locked Loop) circuit 11 in the RF processing circuit 10By the encoder / decoder

15it encodes and decodesand the acquired EFM signal is supplied to H.CPU26 of the exterior via I/F(interface) 16and is stored in the memory measure 26 of H.CPU26.

[0027]The push pull signal of the RF signal acquired from RF amplifier 9 is supplied to the ATIP (Absolute Time In Pregroove) decoder 13 in the RF signal processing circuit 10aargh -- the pregroove by which the bull was carried out -- aarghbul processing is performed and the synchronous interrupt user data and the address decode result of ATIP are given to CPU17.

[0028]Re-write data is given from H-CPU26 and EFM data drives the power laser 6 through RF amplifier 9 and the laser drive circuit 8 via I/F16and the encoder/decoder 15.

[0029]CPU17 has ADC (analog-digital converter)18 and DAC (digital-to-analog converter)19The data which digitized the RF signal via ADC18 from RF amplifier 9 is given to CPU17The analog pattern waveform which serves as identification data (fingerprint peculiar to a recording medium which spaces through CD-R and is written in as art) as security information from CPU17 via DAC19 is supplied.

[0030]In an above-mentioned recording and reproducing devicedrawing 2 and drawing 3 explain the composition which writes identification data (it is described as fingerprint data below) in CD-R1. Although identical codes are given to a corresponding point with drawing 1 by drawing 2 and drawing 3 and duplication explanation is omitteddrawing 2 is a case where laser power control is performedand drawing 3 shows the distribution diagram in the case of also performing focus bias control.

[0031]In drawing 2although it may be included in CPU17the random number generation means 24 is prepared and random data is generated by this random number generation means 24. Supply this random data to DAC19and in order to shake by the desired value of the laser power of the high power laser 6 by the random signal which carried out analogue conversion by DAC19the noninverting terminal of RF amplifier 9 is suppliedHe connects a laser power monitor to an inversion terminaland is trying to drive the high power laser 6 via the laser drive circuit 8.

[0032]In order to shake the amount of focus bias (offset) of the optical pickup 5 by random data in drawing 3 and to write fingerprint data in the recording layer 1bThe random signal obtained from DAC19 is supplied to the inversion terminal of the summing amplifier 25The RF signal acquired via the optical pickup 5 and RF amplifier 9 is supplied to the noninverting terminal of the summing amplifier 25a summing amplifier output is supplied to the optical pickup 5 via the servo circuit 20 and the focus driving circuit 21aand the writing of a fingerprint is performedshaking focus bias.

[0033]The flow chart of drawing 4 thru/or drawing 6 and the wave form chart of drawing 7 and drawing 8 explain operation with the distribution diagram explained by above-mentioned drawing 1 and drawing 2.

[0034]Drawing 4 shows the flow chart at the time of the writing of the fingerprint data of CD-R1. In drawing 4the prescribed position of CD-R1 is accessed by 1st

step S_1 .

[0035] In 2nd step S_2 a random numerical value is generated by the random number generation means 24.

[0036] In 3rd step S_3 laser power is controlled by the random numerical value acquired by 2nd step S_2 like drawing 2 and the fingerprint data which is identification data is written in the prescribed position of CD-R1 in analog.

[0037] In 4th step S_4 writing is stopped at the time of the write end of the predetermined regenerative waveform 29 as shown in drawing 7 and it results in an end.

[0038] Drawing 5 shows the flow chart at the time of registration of the fingerprint data of H-CPU26 and accesses the optical pickup 5 in 1st step ST_1 at the predetermined specified position of CD-R1.

[0039] In 2nd step ST_2 read-out of the fingerprint data written in CD-R1 is started.

[0040] In 3rd step ST_3 the fingerprint data recorded on CD-R1 is changed into digital data via DAC19 and it transmits to H-CPU26.

[0041] By 3rd step ST_3 as fingerprint data, the case where the regenerative waveform 29 like drawing 7 is obtained -- Time t_1, t_2, t_3 and $t_4 \dots t_i \dots t_n$ the digital conversion value by ADC18 of t_n -- respectively -- A_1, A_2, A_3 and $A_4 \dots A_i \dots A_n$ it being considered as A_n and the whole data row being set to W_{vd} and it is considered as data set value $W_i = (t_i, A_n)$ in digital conversion value A_i at the time of time t_i .

[0042] The necessity of normalizing since it differs by reproduction conditions such as a gain dispersion of the drive characteristic aging of CD-R1 etc. produces above-mentioned digital conversion value A_i .

[0043] For example the repetition regenerative waveform 29 shown in drawing 7 of $mT=4T$. If the value after each ADC at the time of being V_1, V_2, V_3 and V_4 is set with pk_1, pk_2, pk_3 and pk_4 as the level of a peak two-piece (Peak to Peak) when it writes in CD-R1 shows drawing 8 Average value $pk\text{-ave}$ of this peak two-piece value $pk_1 - pk_4$ is $pk\text{-ave} = (pk_1 + pk_2 + pk_3 + pk_4) / 4 \dots (1)$

It becomes.

[0044] A_i is normalized with the regeneration level of $4T$ here (Normalize). That is it will be $B = A_i / pk\text{-ave}$ if normalized peak value is made into $B_i \dots (2)$

It can come out and express.

[0045] Next in 4th step ST_4 the normalized above-mentioned regenerative waveform 29 is stored in the nonvolatile memory measure 27 which H-CPU26 has with the management number of CD-R1 and registration is ended for this as the security information of CD-R1 i.e. fingerprint data.

[0046] Although the random pattern i.e. fingerprint data recorded on CD-R1 was incorporated as an analog-spectrum form by ADC and the waveform was stored in H-CPU26 via ADC with above-mentioned composition it may be made to store in H-CPU26 the fingerprint data which binary-ized the random pattern of CD-R1 with the high-speed sample rate quicker than usual.

[0047] Next drawing 6 explains the flow chart of the write-in permission to CD-R1 and disapproval processing. With the recording and reproducing device 28 this flow chart reads the fingerprint data recorded on CD-R1 compares it with the

fingerprint data stored in H-CPU26 and accesses the optical pickup 5 by 1st step STP₁ in a prescribed position.

[0048] In 2nd step STP₂, the lead of the fingerprint data written in CD-R1 is started.

[0049] Although all the data row Wvdt(s) of the fingerprint data shown by drawing 7 with the disk management number of CD-R1 are registered into H-CPU26, this is set to Wvdt₀ and peak value B_i normalized by above-mentioned (2) formulas is made into R_i. Namely $R_i = B_i$ (1 ≤ i ≤ S) ... (3)

S is the number of W_i here.

[0050] In 3rd step STP₃, the recording and reproducing device 28 reads in analog the fingerprint data recorded on CD-R1 read via the optical pickup 5 and transmits all the data row Wvdt(s) which carried out digital conversion via ADC18 to the H-CPU26 side.

[0051] In 4th step STP₄, H-CPU26 takes out fingerprint data Wvdt₀ (set of R_i) of the disk corresponding to the disk management number of CD-R1 from the memory measure 27.

[0052] 5th step STP₅ compares fingerprint data Wvdt (set of B_i) of all the data rows of CD-R1 transmitted by 3rd step STP₃.

[0053] These comparison operations are $R_i + Wdu > B_i > R_i - Wdl$... (4)

Here, it is an acceptable value of the Wdu: upper part. It is an acceptable value of the Wdl: bottom. It becomes.

[0054] When F is made into the total number of B_i (1 ≤ i ≤ S) which fills (4) types now, $\eta = F/S$ is defined and the following conditions are considered at this time. $\eta > C$... (5)

C is an allowable ratio for example is chosen to 70 percent – about 90 percent here.

[0055] It is judged whether it was satisfied with 6th step STP₆ of (5) types. That is, H-CPU26 judges whether comparison data fulfilled the predetermined allowable ratio rate and if (5) types are not filled, the instructions which progress to 7th step STP₇ and forbid the writing of CD-R1 are transmitted to a recording and reproducing device.

[0056] On the other hand, in being satisfied with 6th step STP₆ of (5) types, it accomplishes so that it may progress to 8th step STP₈ and the write-in permission command of CD-R1 may be transmitted to a recording and reproducing device.

[0057] This invention is constituted like the above statement and since it operates an alteration and the identifying method which cannot be forged can be illegally acquired for important electronic files such as the recording medium and recording and reproducing device which cannot be forged and settlement of accounts with easy composition. Since the analog waveform was used as identification data (fingerprint data), the system in which powerful protection is possible is obtained also to electronic authentication.

[0058]

[Effect of the Invention] Since the analog random waveform is recorded as identification data according to the recording medium of this invention, powerful protection is attained with the identification data which is hard to decode as

compared with the case where the identification data which is security information in digital one is processed.

[0059] According to the identifying method of the recording medium of this invention the identifying method which cannot alter or forge easily the electronic file which needs recognition settlement of account etc. is acquired simply.

[0060] If it is a recording and reproducing device which has an optical pickup in which record reproduction is possible for the data of a recording medium according to the recording and reproducing device of the recording medium of this invention the recording and reproducing device which can record identification data will be obtained simply without forming a special device.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a distribution diagram of the recording and reproducing device of this invention.

[Drawing 2] It is a distribution diagram of the laser power control part of this invention.

[Drawing 3] It is a distribution diagram of the focus bias control section of this invention.

[Drawing 4] It is a flow chart of the writing of the identification data to the recording medium of this invention.

[Drawing 5] It is a flow chart at the time of registration of the identification data to the host computer of this invention.

[Drawing 6] It is a flow chart of the write-in permission to the recording medium of this invention and disapproval processing.

[Drawing 7] It is a sample timing wave form chart of the regenerative waveform for explanation of this invention of operation and ADC.

[Drawing 8] It is a calibration regenerative waveform figure of the explanatory view of this invention of operation.

[Description of Notations]

1 [.... A laser drive circuit 9 / An RF amplifier 10 / RF processing circuit 17 / CPU 24 / A random number generation means 25 / A summing amplifier 26 / H-CPU 27 / Memory measure] A recording medium (CD-R) 5 An optical pickup 6 Power laser 8

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-273705
(P2001-273705A)

(43) 公開日 平成13年10月5日 (2001.10.5)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)		
G 1 1 B 19/04	5 0 1	G 1 1 B 19/04	5 0 1 H	5 D 0 4 4	
7/004		7/004	C	5 D 0 6 6	
7/007		7/007		5 D 0 9 0	
19/02	5 0 1	19/02	5 0 1 J		
20/10		20/10	H		
審査請求 未請求 請求項の数 5 O L (全 11 頁)					

(21) 出願番号 特願2000-28053(P2000-28053)

(22) 出願日 平成12年2月4日 (2000.2.4)

(31) 優先権主張番号 特願2000-9381(P2000-9381)

(32) 優先日 平成12年1月18日 (2000.1.18)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 飯田 道彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100080883

弁理士 松隈 秀盛

F ターム (参考) 5D044 BC06 CC04 DE49 DE50 DE52

GK17 HL08

5D066 DA04 DA12 DA16

5D090 AA01 BB04 CC01 DD03 DD05

FF09 FF31 FF41 FF49 GG32

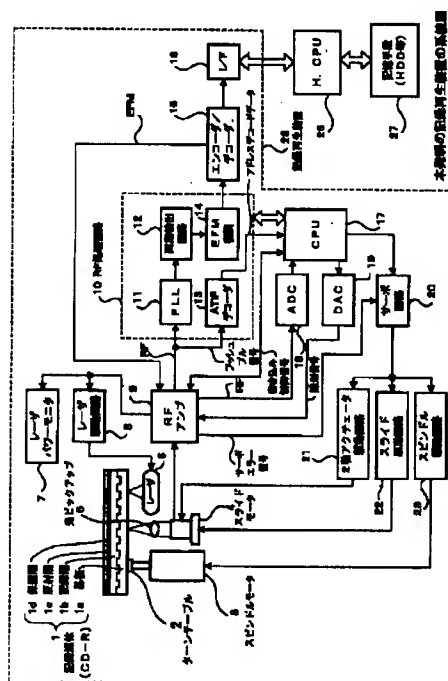
GG33

(54) 【発明の名称】 記録媒体及びその識別方法並びにその記録再生装置

(57) 【要約】

【課題】 書き込み可能な記録媒体への承認、決済等の重要ファイルデータの改竄、偽造を強力に防止する。

【解決手段】 書き込み可能な記録媒体へランダムなアナログ的な波形信号を記録し、識別データ、即ち指紋データとして登録し、この指紋データをホストコンピュータに転送して記録媒体固有の指紋として格納して置き、記録媒体への再書き込み時にホストコンピュータに格納した指紋データと記録媒体の指紋データを比較し、所定比較範囲値内に入ったときのみ書き込み許可を与えるようにした記録媒体及びその識別方法並びに記録媒体の記録再生装置を提供する。



【特許請求の範囲】

【請求項 1】 再書き込み可能な記録媒体であって、上記記録媒体の所定データ記録領域内にランダムな波形パターンを記録し、該記録媒体の識別データとなしたことを特徴とする記録媒体。

【請求項 2】 前記ランダムな波形パターンは乱数発生手段で発生させたランダムデータによってレーザパワー値を所定範囲値内で振って得た識別データであることを特徴とする請求項 1 記載の記録媒体。

【請求項 3】 前記ランダムな波形パターンは乱数発生手段で発生させたランダムデータによってフォーカスバイアス値を所定範囲内で振って得た識別データであることを特徴とする請求項 1 記載の記録媒体。

【請求項 4】 再書き込み可能な記録媒体の所定データ記録領域内にランダムな波形パターンを記録する記録ステップと、上記記録ステップで記録したランダムな波形パターンを取り込んでホス、コンピュータに送出して該ホストコンピュータ内の記憶手段に識別データとして記憶する記憶ステップと、上記記録媒体への書き込み時に上記記録ステップで記録したランダムな波形パターンを読み出し、デジタルデータとして上記ホストコンピュータに送出し、該ホストコンピュータはこの送出されデジタルデータを上記記憶手段内の識別データと比較し、この比較データが所定の範囲内の値であれば該記録媒体への書き込みを許可する比較ステップと、より成ることを特徴とする記録媒体の識別方法。

【請求項 5】 再書き込み可能な記録媒体の所定のデータ書き込み領域内にランダムな波形パターンを記録する記録手段と、

上記記録手段で記録したランダムな波形パターンを再生し、ホストコンピュータに送出する再生手段と、

上記ホストコンピュータに送出した上記ランダムな波形パターンを該ホストコンピュータに記憶して記録媒体の識別データとし、記録媒体の再書き込み時に上記再生手段が該ホストコンピュータに送出したランダムな波形パターンを該ホストコンピュータは該識別データと比較する比較手段とを有し、

上記ホストコンピュータは再書き込み許可又は不許可データを送出するように成したことを特徴とする記録媒体の記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は再書き込み可能な記録媒体及びその識別方法並びにその記録再生装置に係わり、特に、再書き込み可能な記録媒体の記録装置に用いて好適な記録媒体及びその識別方法並びにその記録再生装置に関する。

【0002】

【従来の技術】 従来からコンピュータソフト、映像ソフト、音声ソフト等の各種記録媒体からのコピー或は改竄は比較的容易であるため、これら不正コピーや改竄を防止するための防止措置がとられている。これら防止措置は多くの方法が提案されているが、基本的には記録媒体自体に特異なコードを論理的或は物理的に記録し、これを読み取ることで不正或は正規の記録媒体であるか等の識別を行なっている。

【0003】 例えば、特開平 7-176080 号公報では物理的に記録媒体のデータ記録領域内或は記録領域外に再生光により読み取り可能なパターンコードをセキュリティ情報として記録媒体作成時に形成し、コピーした記録媒体との差別化を図った記録媒体が開示されている。

【0004】 又、特開平 8-153342 号公報には記録媒体管理領域中の内周にあるバッファ領域内に通常のものとは見分けの付かない同一フォーマットで、時間情報の断絶を利用してセキュリティ情報を論理的に記録した記録媒体及びそのチェック装置が開示されている。

【0005】

【発明が解決しようとする課題】 近時、CD-RW (Compact Disc Rewritable)、DVD-RAM (Digital Versatile Disc-RAM)、MO (Magnet Optical disc)、磁気テープ等の再書き込み可能な記録媒体、或は CD-R (Compact Disc Recordable)、DVD-R (Digital Versatile Disc Recordable) 等の WORM (Write Once Read Many optical disc : 追記型光ディスク) 等の記録媒体が広く出回っている。上記したセキュリティ情報でコピーや改竄を防止する様にした記録媒体は再生専用でデジタルデータでセキュリティ情報を管理しているものが多い。

【0006】 上述の再書き込み可能な記録媒体或は WORM の様な記録媒体では例えば、承認、決済、認証等を必要とする重要な事項を記録して電子ファイル化する場合に記録媒体自身に記録が可能であり、且つ不正な改竄或は偽造ができないようにする必要があるが、上述のように物理的にセキュリティ情報としての識別情報を記録媒体に入れる場合は多くの設備を必要とし市販済の記録媒体との間での互換性等も問題となる。

【0007】 一方、論理的にセキュリティ情報としての識別情報を記録媒体に入れる場合にデジタルデータでセキュリティ情報の管理を行なう場合は原理的にはセキュリティ情報が解読され改竄や偽造が可能となる問題があった。

【0008】 本発明は叙上の課題を解消するためになされたもので、識別情報が解読しにくいセキュリティ情報を記録した記録媒体及びその識別方法並びにその記録再生装置を提供しようとするものである。

【0009】

【課題を解決するための手段】 第 1 の本発明の記録媒体

は再書き込み可能な記録媒体であって、この記録媒体の所定データ記録領域内にランダムな波形パターンを記録し、記録媒体の識別データとなしたものである。

【0010】第2の本発明の記録媒体は前記したランダムな波形パターンを乱数発生手段で発生させたランダムデータによってレーザパワー値を所定範囲値内で振って得た識別データを記録したものである。

【0011】第3の本発明の記録媒体は前記ランダムな波形パターンを乱数発生手段で発生させたランダムデータによってフォーカスバイアス値を所定範囲値内で振って得た識別データを記録したものである。

【0012】本発明の記録媒体の識別方法は再書き込み可能な記録媒体の所定データ記録領域内にランダムな波形パターンを記録する記録ステップと、この記録ステップで記録したランダムな波形パターンを取り込んでホストコンピュータに送出して、ホストコンピュータ内の記憶手段に識別データとして記憶する記憶ステップと、記録媒体への書き込み時に記録ステップで記録したランダムな波形パターンを読み出し、デジタルデータとしてホストコンピュータに送出し、ホストコンピュータはこの送出させたデジタルデータを記憶手段内の識別データと比較し、この比較データが所定の範囲内の値であれば記録媒体への書き込みを許可する比較ステップとより成るものである。

【0013】本発明の記録媒体の記録再生装置は再書き込み可能な記録媒体の所定のデータ記録領域内にランダムな波形パターンを記録する記録手段と、この記録手段で記録したランダムな波形パターンを再生し、ホストコンピュータに送出する再生手段と、ホストコンピュータに送出したランダムな波形パターンをホストコンピュータは記憶して記録媒体の識別データとし、記録媒体の再書き込み時に再生手段がホストコンピュータに送出したランダムな波形パターンをホストコンピュータは識別データと比較する比較手段とを有し、ホストコンピュータは再書き込み許可又は不許可データを送出するように成したものである。

【0014】上述の第1乃至第3の記録媒体によればアナログ的なランダム波形を識別データとして記録しているためデジタル的にセキュリティ情報である識別データを処理する場合に比較して解読し難い識別データによって強力なプロテクトが可能となる。

【0015】又、上述の記録媒体の識別方法によれば承認、決済等を必要とする電子ファイルを容易に改竄或は偽造できない識別方法が簡単に得られる。

【0016】更に、上述の記録媒体の記録再生装置によれば記録媒体のデータを記録再生可能な光ピックアップを有する記録再生装置であれば、特別な装置を設けずに簡単に識別データを記録可能な記録再生装置が得られる。

【0017】

【発明の実施の形態】以下、本発明の1形態例を図1乃至図8によって説明する。

【0018】図1は本発明の記録再生装置の系統図を示すものであり、記録媒体として追記型光ディスクであるCD-Rの記録再生装置について説明する。

【0019】図1に於いて、記録再生装置28はホストコンピュータ（以下、H. CPUと記す）26にバスを介して接続され、H. CPU26はハードディスクドライブ（HDD）等の記憶手段27を有している。

【0020】記録再生装置28内には記録媒体（以下CD-Rと記す）1を有し、このCD-R1は合成樹脂基板1a上にプリグループを形成すると共にシアン系の色素等の記録層1b上に金等の反射層1cを形成し、この反射層1c上を保護層1dによって被覆している。

【0021】CD-R1はターンテーブル2上に載置され、スピンドルモータ3で回転され、スピンドルモータ3はサーボ回路20及びスピンドル駆動回路23を介して駆動制御される。

【0022】光ピックアップ5とハイパワーレーザ6はスライドモータ4によりCD-R1の輻方向に移動可能となされている。スライドモータ4はサーボ回路20とスライド駆動回路22を介して光ピックアップ5やハイパワーレーザ6をスライド制御する。

【0023】ハイパワーレーザ6はCD-Rへの再書き込み時にCPU17から書き込み制御信号がRFアンプ9を経て、レーザ駆動回路8に供給され、ハイパワーレーザ6を駆動制御すると共にレーザパワーモニタ7でハイパワーレーザ6のパワーがモニタされる。

【0024】光ピックアップ5はフォーカス及びトラッキングの2軸方向の制御がサーボ回路20と2軸アクチュエータ駆動回路21を介して駆動制御される。

【0025】サーボ回路20にはRFアンプ9からのRF信号とCPU17からの制御信号が供給されている。光ピックアップ5でピックアップされた反射光は電気信号に変換されRFアンプ9を介してRF信号を出力し、RF処理回路10に供給される。

【0026】RF信号はRF処理回路10内のPLL（Phase Locked Loop）回路11を介して同期検波回路12で同期検波後にEFM（8-14変調）復調し、エンコーダ/デコーダ15でエンコード及びデコードし、得られたEFM信号はI/F（インタフェース）16を介して外部のH. CPU26に供給され、H. CPU26の記憶手段26に格納される。

【0027】RFアンプ9から得たRF信号のプッシュプル信号はRF信号処理回路10内のATIP（Absolute Time In Pregroove）デコーダ13に供給され、ウォーブルされたプリグループでウォーブル処理が施されATIPの同期割り込みデータとアドレスデコード結果がCPU17に与えられる。

【0028】再書き込みデータはH-CPU26から与

えられ、I/F16及びエンコーダ/デコーダ15を介してEFMデータはRFアンプ9及びレーザ駆動回路8を経てパワーレーザ6を駆動する。

【0029】更にCPU17はADC（アナログデジタル変換器）18及びDAC（デジタルアナログ変換器）19を有し、RFアンプ9からADC18を介してRF信号をデジタル化したデータがCPU17に与えられ、CPU17からDAC19を介してセキュリティ情報としての識別データ（CD-Rに透し技術として書き込まれる記録媒体固有の指紋）となるアナログ的なパターン波形が供給される。

【0030】上述の記録再生装置に於いて、識別データ（以下指紋データと記す）をCD-R1に書き込む構成を図2及び図3で説明する。図2及び図3で図1との対応部分には同一符号を付して重複説明を省略するが、図2はレーザパワー制御を行う場合であり、図3はフォーカスバイアス制御も行う場合の系統図を示している。

【0031】図2では、CPU17内に包含されていてもよいが、乱数発生手段24を用意し、この乱数発生手段24でランダムデータを発生させる。このランダムデータをDAC19に供給して、DAC19でアナログ変換したランダム信号でハイパワーレーザ6のレーザパワーの目標値で振るためにRFアンプ9の非反転端子に供給し、反転端子にレーザパワーモニタを接続し、レーザ駆動回路8を介してハイパワーレーザ6を駆動する様にしている。

【0032】図3では光ピックアップ5のフォーカスバイアス（オフセット）量をランダムデータで振って指紋データを記録層1bに書き込むために、DAC19から得たランダム信号を加算アンプ25の反転端子に供給し、光ピックアップ5とRFアンプ9を介して得たRF信号を加算アンプ25の非反転端子に供給し、加算アンプ出力をサーボ回路20とフォーカス駆動回路21aを介して光ピックアップ5に供給して、フォーカスバイアスを振りながら指紋の書き込みが行われる。

【0033】上述の図1及び図2で説明した系統図での動作を図4乃至図6のフローチャート及び図7と図8の波形図により説明する。

【0034】図4はCD-R1への指紋データの書き込

$$pk \cdot ave = (pk1 + pk2 + pk3 + pk4) / 4 \dots (1)$$

となる。

【0044】ここで A_j を4Tの再生レベルで正規化(Normalize)する。即ち、正規化された波高値を B_j とすれば

$$B_j = A_j / pk \cdot ave \dots (2)$$

で表すことが出来る。

【0045】次に第4ステップST4では上述の正規化した再生波形29をCD-R1の管理番号と共にH-CPU26が有する不揮発性の記憶手段27に格納し、これをCD-R1のセキュリティ情報、即ち、指紋データ

み時のフローチャートを示すものである。図4に於いて、第1ステップS1ではCD-R1の所定位置にアクセスする。

【0035】第2ステップS2では乱数発生手段24によって、ランダム数値を発生させる。

【0036】第3ステップS3では第2ステップS2で得たランダム数値で図2の様にレーザパワーを制御して識別データである指紋データをアナログ的にCD-R1の所定位置に書き込みを行う。

【0037】第4ステップS4では例えば図7に示す様な所定の再生波形29の書き込み終了時に書き込みを停止してエンドに至る。

【0038】図5はH-CPU26への指紋データの登録時のフローチャートを示すもので第1ステップST1では光ピックアップ5をCD-R1の所定の指定位置にアクセスする。

【0039】第2ステップST2ではCD-R1に書き込まれた指紋データの読み出しを開始する。

【0040】第3ステップST3ではCD-R1に記録された指紋データをDAC19を介してデジタルデータに変換してH-CPU26に転送する。

【0041】第3ステップST3で例えば指紋データとして図7の如き再生波形29が得られた場合に時刻 $t_1, t_2, t_3, t_4 \dots t_j \dots t_n$ のADC18によるデジタル変換値を夫々 $A_1, A_2, A_3, A_4 \dots A_j \dots A_n$ とし、データ列全体を $Wvd t$ とし、時刻 t_j の時のデジタル変換値 A_j でのデータセット値 $W_j = (t_j, A_n)$ とする。

【0042】上述のデジタル変換値 A_j はゲイン等の再生条件や駆動特性のばらつきやCD-R1の経時変化等で異なってくるので正規化を施す必要が生ずる。

【0043】例えば $mT = 4T$ の図7に示した繰り返し再生波形29をCD-R1に書き込んだ時のピークツウピース(Peak to Peak)のレベルが図8に示す様に V_1, V_2, V_3, V_4 であった時の夫々のADC後の値を $pk1, pk2, pk3, pk4$ とおくと、このピークツウピース値 $pk1 \sim pk4$ の平均値 $pk \cdot ave$ は、

として登録を終了する。

【0046】上述の構成ではCD-R1に記録したランダムなパターン即ち、指紋データをADCでアナログ波形として取り込み、その波形をADCを介してH-CPU26に格納したが、CD-R1のランダムなパターンを通常より速い高速サンプルレートで2値化した指紋データをH-CPU26に格納する様にしてもよい。

【0047】次にCD-R1への書き込み許可及び不許可処理のフローチャートを図6で説明する。このフローチャートは記録再生装置28によってCD-R1に記録

した指紋データを読み出し、H-CPU26に格納した指紋データと照合を行うもので第1ステップSTP₁では光ピックアップ5を所定位置にアクセスする。

【0048】第2ステップSTP₂ではCD-R1に書き込んだ指紋データのリードを開始する。

【0049】H-CPU26にはCD-R1のディスク管理番号と共に図7で示した指紋データの全データ列Wvd_tが登録されているが、これをWvd_{t0}とし、上述の(2)式で正規化した波高値B_iをR_iとする。即ち、

$$R_i = B_i \quad (1 \leq i \leq S) \quad \dots (3)$$

ここでSはW_iの個数である。

【0050】第3ステップSTP₃において、記録再生装置28は光ピックアップ5を介して読み出したCD-R1に記録された指紋データをアナログ的に読み出し、ADC18を介してデジタル変換した全データ列Wvd_tをH-CPU26側に転送する。

【0051】第4ステップSTP₄において、H-CPU26はCD-R1のディスク管理番号に対応するディスクの指紋データWvd_{t0} (R_iの集合)を記憶手段27から取り出す。

【0052】第5ステップSTP₅では第3ステップSTP₃で転送されて来たCD-R1の全データ列の指紋データWvd_t (B_iの集合)とを比較する。

【0053】この比較動作は

$$R_i + Wdu > B_i > R_i - Wdl \quad \dots (4)$$

ここで、Wdu：上側の許容値 Wdl：下側の許容値である。となる。

【0054】今、Fを(4)式を満たすB_i (1 ≤ i ≤ S)のトータル個数とした時 $\eta = F/S$ を定義し、この時、以下の条件を考える。

$$\eta > C \quad \dots (5)$$

ここでCは許容比率であり例えば7割～9割程度に選択される。

【0055】第6ステップSTP₆では(5)式が満足されたか否かを判断する。即ち、比較データが所定の許容比率割合を満たしたかどうかをH-CPU26は判断し、(5)式を満たしていなければ第7ステップSTP₇に進んでCD-R1への書き込みを禁止する指令を記録再生装置に転送する。

【0056】一方、第6ステップSTP₆で(5)式を満足する場合には第8ステップSTP₈に進んでCD-R1への書き込み許可指令を記録再生装置に転送する様

に成される。

【0057】本発明は叙上の様に構成し、且つ動作するので偽造不可能な記録媒体及び記録再生装置並びに決済等の重要な電子ファイルを不正に改竄や偽造できない識別方法を簡単な構成で得ることが出来、アナログ的な波形を識別データ(指紋データ)としたので電子認証に対しても強力なプロテクト可能なシステムが得られる。

【0058】

【発明の効果】本発明の記録媒体によればアナログ的なランダム波形を識別データとして記録しているためデジタル的にセキュリティ情報である識別データを処理する場合に比較して解読し難い識別データによって強力なプロテクトが可能となる。

【0059】又、本発明の記録媒体の識別方法によれば承認、決済等を必要とする電子ファイルを容易に改竄或は偽造できない識別方法が簡単に得られる。

【0060】更に、本発明の記録媒体の記録再生装置によれば記録媒体のデータを記録再生可能な光ピックアップを有する記録再生装置であれば、特別の装置を設けずに簡単に識別データを記録可能な記録再生装置が得られる。

【図面の簡単な説明】

【図1】本発明の記録再生装置の系統図である。

【図2】本発明のレーザパワー制御部の系統図である。

【図3】本発明のフォーカスバイアス制御部の系統図である。

【図4】本発明の記録媒体への識別データの書き込みのフローチャートである。

【図5】本発明のホストコンピュータへの識別データの登録時のフローチャートである。

【図6】本発明の記録媒体への書き込み許可、不許可処理のフローチャートである。

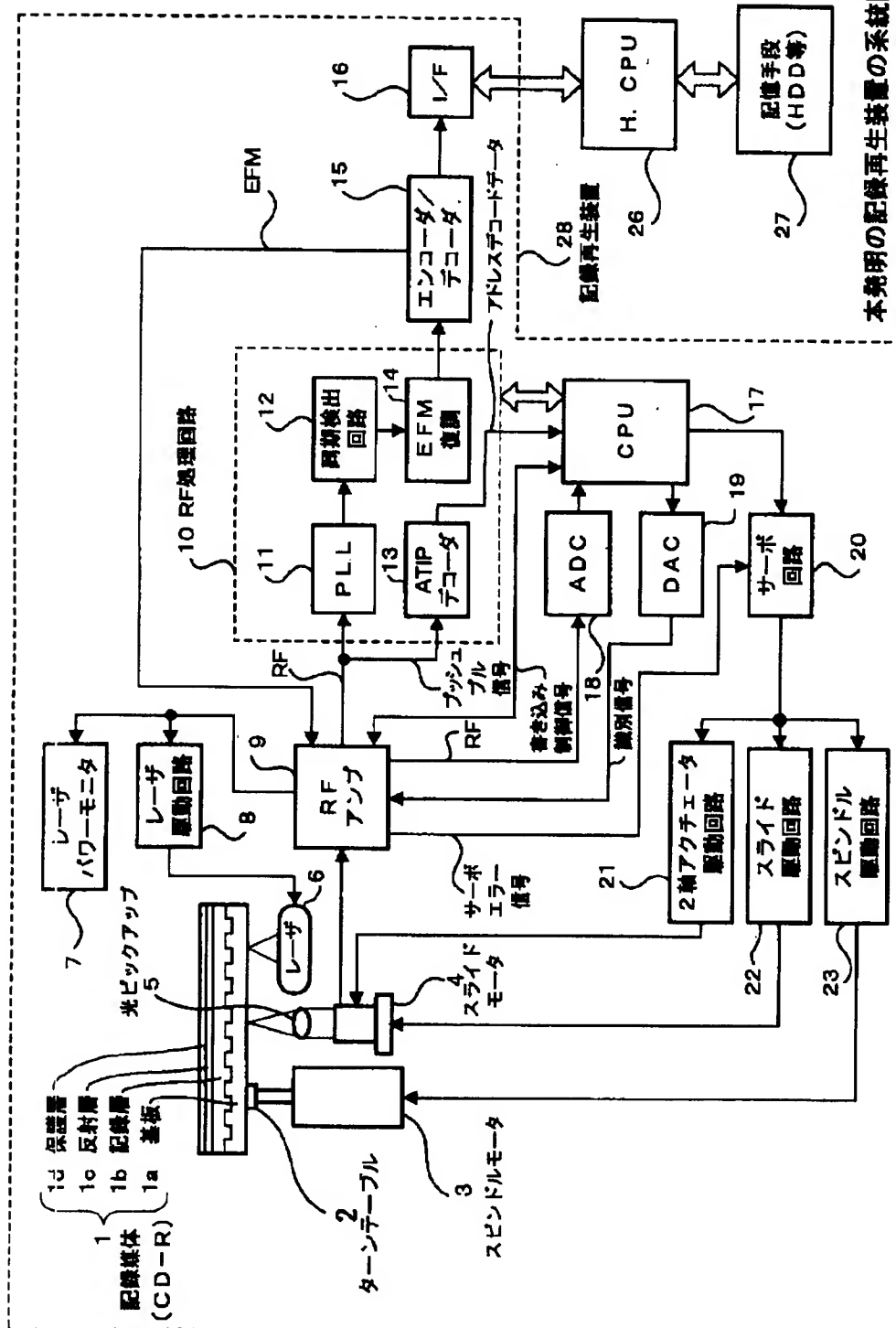
【図7】本発明の動作説明用の再生波形とADCのサンプルタイミング波形図である。

【図8】本発明の動作説明図のキャリブレーション再生波形図である。

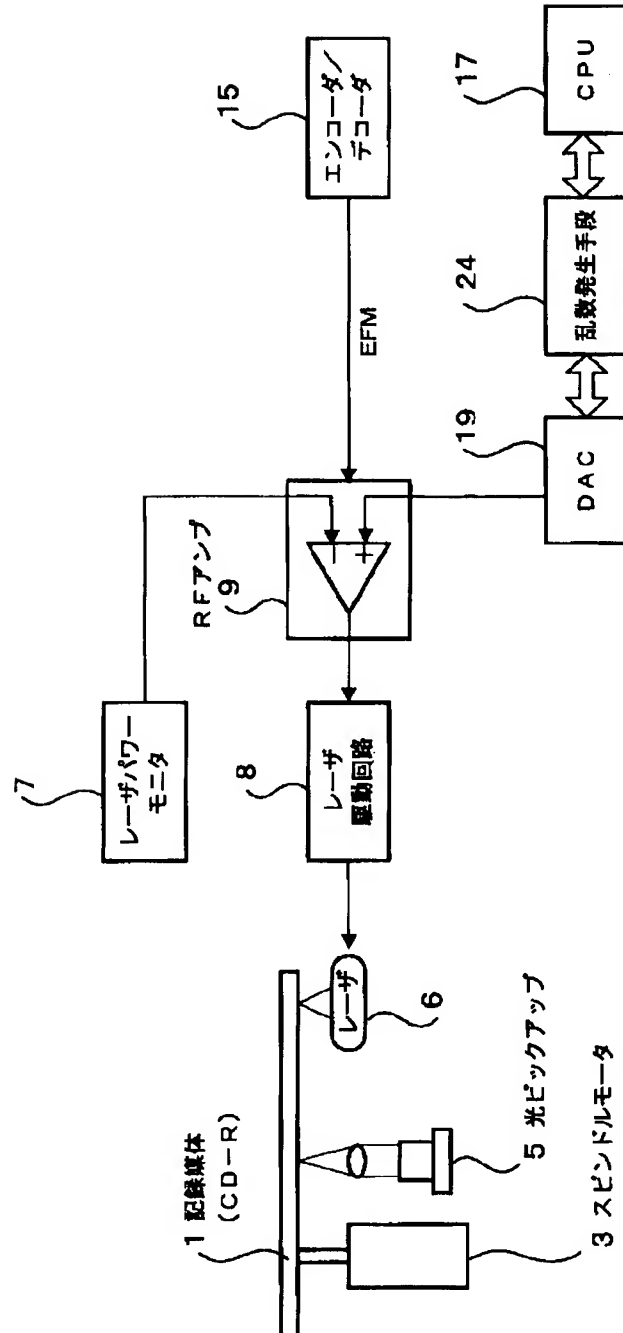
【符号の説明】

1……記録媒体(CD-R)、5……光ピックアップ、6……パワーレーザ、8……レーザ駆動回路、9……RFアンプ、10……RF処理回路、17……CPU、24……乱数発生手段、25……加算アンプ、26……H-CPU、27……記憶手段

本発明の記録再生装置の系統図

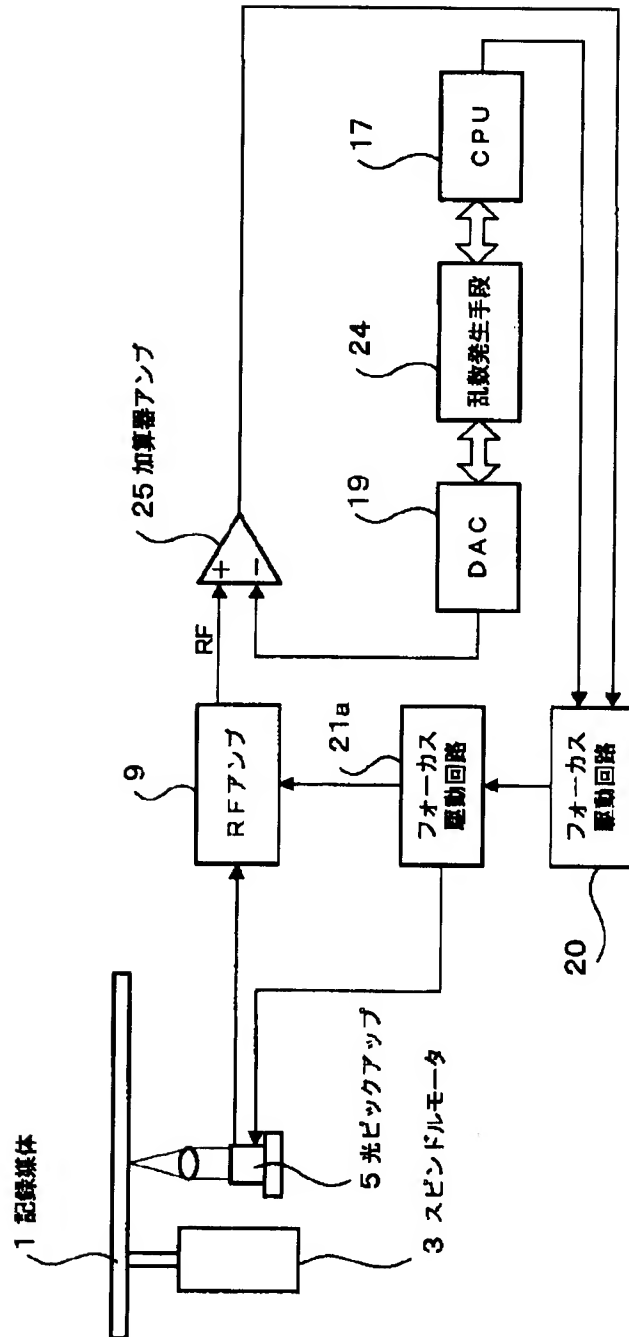


【図2】



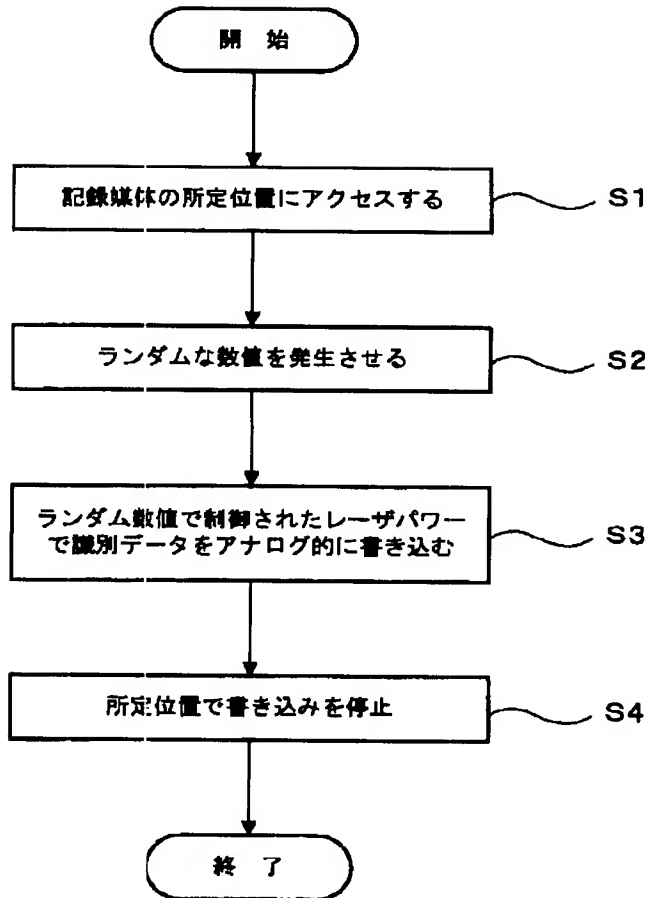
レーザーパワー制御部の系統図

【図3】



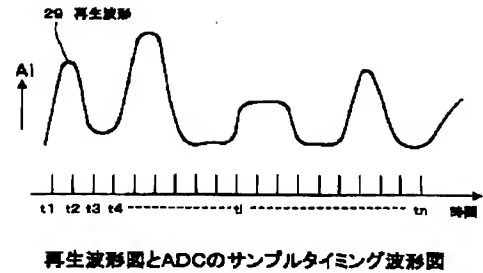
フォーカスバイアス制御部の系統図

【図4】

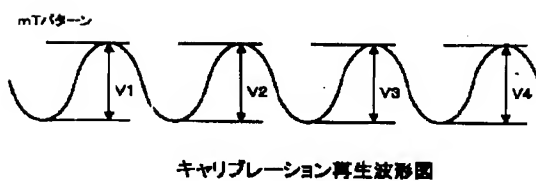


記録媒体への識別データの
書き込みのフローチャート

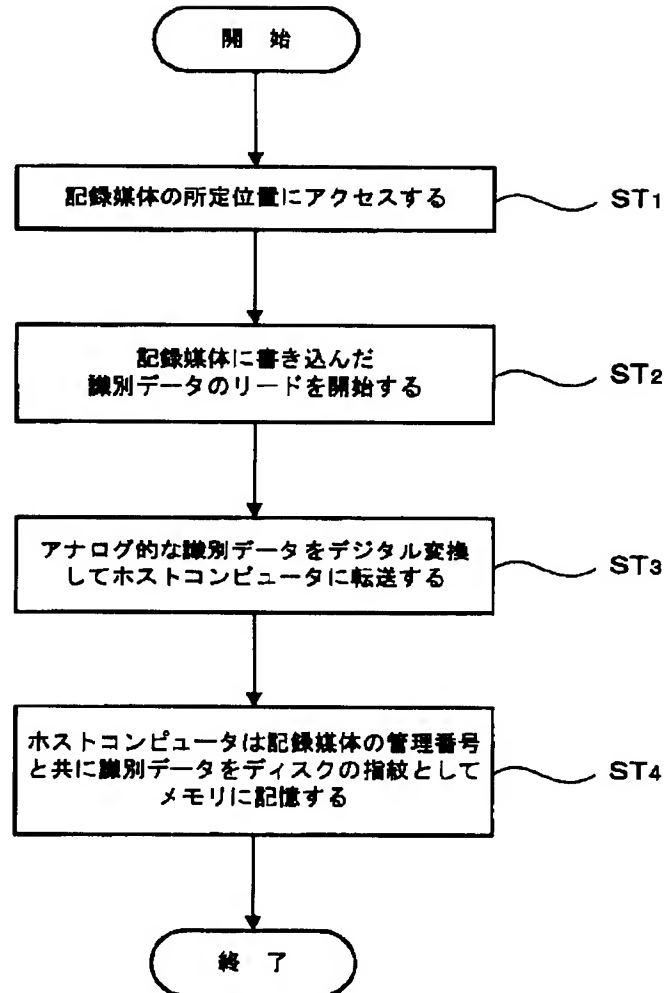
【図7】



【図8】

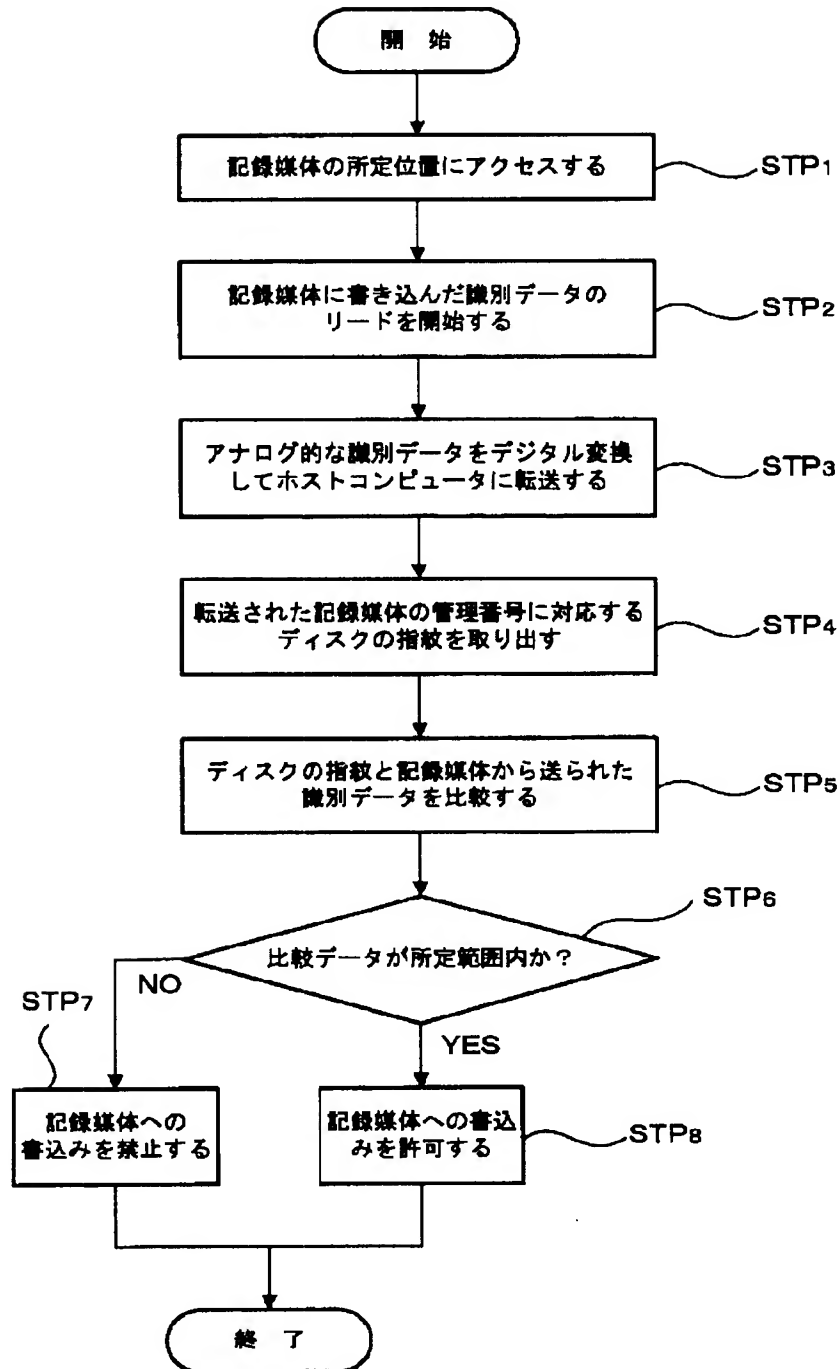


【図5】



ホストコンピュータへの識別データの
登録時のフローチャート

【図6】



記録媒体への書き込み許可不許可処理のフローチャート